UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/379,791	08/24/1999	HIDEO SHIMIZU	04329.2151	1716

22852 7590 07/03/2003

FINNEGAN, HENDERSON, FARABOW, GARRETT & DUNNER LLP
1300 I STREET, NW
WASHINGTON, DC 20005

EXAMINER	
SMITHERS, MATTHEWS	
ART UNIT	**PAPER NUMBER**
2134	6

DATE MAILED: 07/03/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No. 09/379,791	Applicant(s) SHIMIZU ET AL.	
	Examiner Matthew B Smithers	Art Unit 2134	

-- Th MAILING DATE of this communication app ars on the cov r sh et with th correspondence addr ss --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *24 August 1999* .

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-14* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-14* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *24 August 1999* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11)☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

If approved, corrected drawings are required in reply to this Office action.

12)☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____ .

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

14)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

a) ☐ The translation of the foreign language provisional application has been received.

15)☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☒ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) *5* .
4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other:

DETAILED ACTION

Priority

Receipt is acknowledged of papers submitted under 35 U.S.C. 119(a)-(d), which papers have been placed of record in the file.

Information Disclosure Statement

The information disclosure statement filed August 24, 1999 has been placed in the application file and the information referred to therein has been considered as to the merits.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

Claims 1-14 are rejected under 35 U.S.C. 102(b) as being anticipated by U.S. patent 5,594,797 granted to Alanara et al.

Regarding claim 1, Alanara meets the claimed limitations as follows:

"A data processor in which at least one of encryption of a plain text to a cipher text by using an encryption key and decryption of a cipher text to a plain text by using a decryption key is performed, comprising:

a key converting section in which a plurality of key conversion functions which are involution functions, and which conduct key conversions to output extended keys based on one of the encryption key and the decryption key and results of key conversion of one of the encryption key and the decryption key are sequentially connected, and results of the key conversion are in an order or in another order reverse to the order transferred between the key conversion functions; and

a data randomize section in which at least one processing of encryption of the plain text to the cipher text and decryption of the cipher text to the plain text is performed by using the extended keys output from the key conversion section." see column 6, lines 44-65; column 7, lines 35 to column 8, line 38; column 8, lines 57-67 and column 9, lines 28-67.

Regarding claim 2, Alanara meets the claimed limitations as follows:
"A data processor according claim 1, wherein the data randomize section includes a plurality of round functions which are involution functions and which perform at least one of encryption and decryption by using the extended keys, the plurality of round functions are sequentially connected, and results of the processing by the round functions are transferred in an order or in another order reverse to the order transferred between the plurality of round functions." see column 8, line 57 to column 10, line 56.

Regarding claim 3, Alanara meets the claimed limitations as follows:
"A data processor according to claim 1, wherein the key conversion functions not only take first keys and results of conversion of the first keys as objects to be processed in the key conversion, but also perform the key conversion by using a second key." see

column 6, lines 44-58; column 7, lines 35 to column 8, line 38; and column 8, lines 57-67.

Regarding claim 4, Alanara meets the claimed limitations as follows:

"A data processor according to claim 3, wherein the second key is included in at least one of the encryption key and the decryption key." see column 6, lines 44-58; column 7, lines 35 to column 8, line 38; and column 8, lines 57-67.

Regarding claim 5, Alanara meets the claimed limitations as follows:

"A data processor according to claim 4, wherein the second key has different types of keys, at least one of the encryption key and the decryption key includes the different types of keys and at least one of the encryption key and the decryption key is variable in length." see column 6, lines 44-58; column 7, lines 35 to column 8, line 38; and column 8, lines 57-67.

Regarding claim 6, Alanara meets the claimed limitations as follows:

6. A data processor according to claim 2, wherein the key conversion functions include round functions same as that of the data randomize section." see column 8, line 57 to column 10, line 56.

Regarding claim 7, Alanara meets the claimed limitations as follows:

"A communication system comprising:

one communication device which includes a data processor according to claim 1 and holds one key which serves as the encryption key and the decryption key; and

another device which includes a data processor according to claim 1 and holds other key which serves as the encryption key and the decryption key, and which is a

result of key conversion of the one key in the key conversion section of the another device." see column 2, lines 58-66 and column 3, lines 33-41.

Claim 8 is a computer readable medium claim that is substantially equivalent to data processor claim 1. Therefore claim 8 is rejected by a similar rationale.

Claims 9-13 are computer readable medium claims that are substantially equivalent to data processor claims 2-6. Therefore claims 2-6 are rejected by a similar rationale.

Regarding claim 14, Alanara meets the claimed limitations as follows:

"A data transformation apparatus comprising: a key transformation section for outputting a second key and a third key by using an involution function based on inputted first key and for outputting the first key and a fourth key by using the involution function based on inputted second key, wherein the third key is used when first data is transformed to second data and the fourth key is used when the second data is transformed to the first data." see column 6, lines 44-65; column 7, lines 35 to column 8, line 38; column 8, lines 57-67 and column 9, lines 28-67.

Conclusion

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Matthew B Smithers whose telephone number is (703) 308-9293. The examiner can normally be reached on Monday-Friday (9:00-5:30) EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are (703)

746-7239 for regular communications and (703) 746-7238 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-3900.

Matthew B Smithers
Primary Examiner
Art Unit 2134

June 26, 2003